IN THE CLAIMS:

- 1 (Original) An elliptic curve arithmetic operation device for performing one of an
- addition and a doubling on an elliptic curve E: y = 2 = f(x) on a residue class ring of polynomials
- 3 in two variables α and β , moduli of the residue class ring being polynomials β { 2- $f(\alpha)$ and $h(\alpha)$,
- 4 where $f(\alpha) = \alpha$ { $3 + a\alpha + b$, a and b are constants, and $h(\alpha)$ is a polynomial in the variable α , the
- 5 elliptic curve arithmetic operation device comprising:
- acquiring means for acquiring affine coordinates of at least one point on the
- 7 elliptic curve E and operation information indicating one of the addition and the doubling, from
- 8 an external source;
- 9 transforming means for performing a coordinate transformation on the acquired
- 10 affine coordinates to generate Jacobian coordinates, the coordinate transformation being
- transforming affine coordinates $(\phi(\alpha), \beta x \phi, (\alpha))$ of a given point on the elliptic curve E using
- 12 polynomials
- 13 $X(\alpha) = f(\alpha) x \phi(\alpha)$
- $Y(\alpha) = f(\alpha) \quad \{ 2x\varphi \ (\alpha) \}$
- 15 $Z(\alpha)=1$
- into Jacobian coordinates $(X(\alpha) : Y(\alpha) : \beta x Z(\alpha)), \phi(\alpha)$ and $\phi(\alpha)$ being
- 17 polynomials; and
- operating means for performing one of the addition and the doubling indicated by
- 19 the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian
- 20 coordinates of a point on the elliptic curve E.

1	2. (Original) The elliptic curve arithmetic operation device of Claim 1,
2	wherein the acquiring means
3	(a) in a first case acquires affine coordinates of two different points on the
4	elliptic curve E and operation information indicating the addition, and
5 .	(b) in a second case acquires affine coordinates of a single point on the elliptic
6	curve E and operation information indicating the doubling,
7	wherein the transforming means
8	(a) in the first case performs the coordinate transformation on the acquired
9	affine coordinates of the two different points to generate Jacobian coordinates of the two
10	different points, and
11	(b) in the second case performs the coordinate transformation on the acquired
12	affine coordinates of the single point to generate Jacobian coordinates of the single point, and
13	wherein the operating means
14	(a) in the first case performs the addition indicated by the acquired operation
15	information on the generated Jacobian coordinates of the two different points to obtain the
16	Jacobian coordinates of the point on the elliptic curve E , and
17	(b) in the second case performs the doubling indicated by the acquired
18	operation information on the generated Jacobian coordinates of the single point to obtain the
19	Jacobian coordinates of the point on the elliptic curve E .
1	3. (Currently Amended) The elliptic curve arithmetic operation device of Claim 2,
2	wherein in the first case
3	the acquiring means acquires affine coordinates
1	$\frac{1}{(X \cup A) - B \times Y \cup \{\alpha\})} (\phi_{1}(\alpha) - B \times \phi_{2}(\alpha))$

5 $(X2(\alpha), \beta x Y 2 - (\alpha)) (\phi_2 - (\alpha), \beta x \phi_2 - (\alpha))$ of the two different points on the elliptic curve E and the operation information 6 7 indicating the addition, the transforming means performs the coordinate transformation on the acquired 8 9 affine coordinates of the two different points to generate Jacobian coordinates 10 $(X1(\alpha):Y1(\alpha):\beta xZ1(\alpha))$ 11 $(X2(\alpha):Y2(\alpha):\beta xZ2(\alpha))$ of the two different points, and 12 the operating means computes 13 $U1(\alpha) = X1(\alpha) \times Z2(\alpha)$ { 2 14 $U2(\alpha) = X2(\alpha) \times Z1(\alpha)$ { 2 15 $SI(\alpha) = YI(\alpha) xZ2(\alpha)$ { 3 16 $S2(\alpha) = Y2(\alpha) \times Z1(\alpha)$ { 3 17 $H(\alpha) = U2(\alpha) - U1(\alpha)$ 18 19 $r(\alpha) = S2(\alpha) - S1(\alpha)$ 20 and computes $X3(\alpha) = -H(\alpha) \{ 3-2xUI(\alpha)xH(\alpha) \} \{ 2+r(\alpha) \}$ 21 $Y3(\alpha) = -S1(\alpha) xH(\alpha) \{ 3+r(\alpha) x (U1(\alpha)xH(\alpha) \} \{ 2-X3(\alpha) \}$ 22 $Z3(\alpha)=Z1(\alpha) xZ2(\alpha) xH(\alpha)$ 23 to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta xZ3(\alpha))$ of the point on the elliptic 24 25 curve E.

1	4.	(Currently Amended) The elliptic curve arithmetic operation device of Claim 2,
2		wherein in the second case
3		the acquiring means acquires affine coordinates
4		$\frac{(XI(\alpha), \beta xYI(\alpha))}{(\phi_l(\alpha), \beta x \phi_l(\alpha))}$
5		of the single point on the elliptic curve E and the operation information indicating
6	the doubling,	
7		the transforming means performs the coordinate transformation on the acquired
8	affine coordin	nates of the single point to generate Jacobian coordinates
9		$(XI(\alpha):YI(\alpha):\beta xZI(\alpha))$
10		of the single point, and
11		the operating means computes
12		$S(\alpha) = 4 xXI(\alpha)xYI(\alpha) $ { 2
13		$M(\alpha) = 3xXI(\alpha) \{ 2 + \alpha xZI(\alpha) \} \{ 4xf(\alpha) \} $
14		$T(\alpha) = -2xS(\alpha) + M(\alpha) \{ 2 $
15		and computes
16		$X3(\alpha)=T(\alpha)$
17		$Y3(\alpha) = -8xY1(\alpha) \left\{ 4 + M(\alpha)x(S(\alpha) - T(\alpha)) \right\}$
18		$Z3(\alpha) = 2xYI(\alpha)xZI(\alpha)$
19		to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta xZ3(\alpha))$ of the point on the elliptic
20	curve E.	

1	5.	(Curre	ently Amended) The elliptic curve arithmetic operation device of Claim 2,		
2		where	in the acquiring means		
3		(a)	in the first case acquires affine coordinates		
4			$\frac{(XI(\alpha), \beta xYI(\alpha))}{(\phi_1(\alpha), \beta x \phi_1(\alpha))}$		
5			$\frac{(X_2(\alpha), \beta x Y_2(\alpha))}{(\phi_2(\alpha), \beta x \varphi_2(\alpha))}$		
6		of the	two different points on the elliptic curve E and the operation information		
7	indicating the addition, and				
8		(b)	in the second case acquires affine coordinates		
9			$(XI(\alpha), \beta xYI(\alpha)) (\phi_1(\alpha), \beta x \phi_1(\alpha))$		
10		of the	single point on the elliptic curve E and the operation information indicating		
11	the doubling,				
12 ·		where	in the transforming means		
13		(a)	in the first case performs the coordinate transformation on the acquired		
14	affine coordinates of the two different points to generate Jacobian coordinates				
15			$(XI(\alpha):YI(\alpha):\beta xZI(\alpha))$		
16			$(X2(\alpha):Y2(\alpha):\beta xZ2(\alpha))$		
17		of the	two different points, and		
18		(b)	in the second case performs the coordinate transformation on the acquired		
19	affine coordin	ates of	the single point to generate Jacobian coordinates		
20			$(XI(\alpha):YI(\alpha):\beta xZI(\alpha))$		
21		of the	single point, and		
22 .		where	in the operating means		

```
in the first case computes
23
                              (a)
                                        U1(\alpha) = X1(\alpha)xZ2(\alpha) { 2
24
                                        U2(\alpha) = X2(\alpha)xZ1(\alpha) { 2
25
                                        SI(\alpha) = YI(\alpha)xZ2(\alpha) { 3
26
                                        S2(\alpha) = Y2(\alpha)xZ1(\alpha) { 3
27
28
                                        H(\alpha) = U2(\alpha) - U1(\alpha)
                                        r(\alpha) = S2(\alpha) - S1(\alpha)
29
30
                              and computes
                                        X3(\alpha) = -H(\alpha) \{ 3-2xU1(\alpha)xH(\alpha) \} \{ 2+r(\alpha) \} 
31
                                        Y3(\alpha) = -S1(\alpha)xH(\alpha) \quad \{ 3 + r(\alpha)x(U1(\alpha)xH(\alpha) \mid 2 - X3(\alpha)) \}
32
33
                                        Z3(\alpha) = Z1(\alpha) xZ2(\alpha)xH(\alpha)
                              to obtain Jacobian coordinates (X3(\alpha):Y3(\alpha):\beta xZ3(\alpha)) of the point on the elliptic
34
35
        curve E, and
                              (b)
                                        in the second case computes
36
                                        S(\alpha) = 4xXI(\alpha)xYI(\alpha) { 2
37
                                        M(\alpha) = 3xXI(\alpha) \{ 2 + \alpha xZI(\alpha) \} \{ 4xf(\alpha) \} \{ 2 + \alpha xZI(\alpha) \} 
38
39
                                        T(\alpha) = -2xS(\alpha) + M(\alpha)  { 2
40
                              and computes
                                        X3(\alpha) = T(\alpha)
41
                                        Y3(\alpha) = -8xYl(\alpha) \{ 4 + M(\alpha)x(S(\alpha) - T(\alpha)) \}
42
                                        Z3(\alpha) = 2xYI(\alpha)xZI(\alpha)
43
                              to obtain the Jacobian coordinates (X3(\alpha):Y3(\alpha):\beta xZ3(\alpha)) of the point on the
44
45
         elliptic curve E.
```

- 1 6. (Original) An elliptic curve order computation device for computing an order of 2 an elliptic curve according to a Schoof-Elkies-Atkin algorithm, comprising the elliptic curve 3 arithmetic operation device of Claim 1.
- 7. (Original) The elliptic curve order computation device of Claim 6 comprising the elliptic curve arithmetic operation device of Claim 2.
 - 8. (Original) The elliptic curve order computation device of Claim 7 comprising the elliptic curve arithmetic operation device of Claim 5.

9-22. (Cancelled)

1

2

1

1

2

3

4

5

6

7

8

9

10

- 23. (Currently Amended) An elliptic curve arithmetic operation method used in an elliptic curve arithmetic operation device equipped with an acquiring means, a transforming means, and an operating means, for performing one of an addition and a doubling on an elliptic curve $E: y \ \{2=f(x) \text{ on a residue class ring of polynomials in two variables } \alpha \text{ and } \beta, \text{ moduli of the residue class ring being polynomials } \beta \ \{2-f(\alpha) \text{ and } h(\alpha), \text{ where } f(\alpha)=\alpha \ \{3+a\alpha+b, a \text{ and } b \text{ are constants, and } h(\alpha) \text{ is a polynomial in the variable } \alpha, \text{ the elliptic curve arithmetic operation method comprising:}$
- an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;
- a transforming step performed by the transforming means, for performing a coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates,

the coordinate transformation being transforming affine coordinates $(\phi(\alpha), \beta x \phi(\alpha))$ of a given point on the elliptic curve E using polynomials

 $X(\alpha) = f(\alpha)x\phi(\alpha)$

16
$$Y(\alpha) = f(\alpha) \{ 2x\varphi(\alpha) \}$$

 $17 Z(\alpha) = 1$

into Jacobian coordinates $(X(\alpha) : Y(\alpha) : \beta x Z(\alpha))$, ϕ (α) and ϕ (α) being polynomials; and

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

24. (Cancelled)

25. (Original) A computer-readable storage medium storing an elliptic curve arithmetic operation program used in an elliptic curve arithmetic operation device equipped with acquiring means, transforming means, and operating means, for performing one of an addition and a doubling on an elliptic curve E: $y \in 2=f(x)$ on a residue class ring of polynomials in two variables α and β , moduli of the residue class ring being polynomials $\beta \in 2-f(\alpha)$ and $h(\alpha)$, where $f(\alpha) = \alpha \in 3+a\alpha+b$, α and α are constants, and α is a polynomial in the variable α , the elliptic curve arithmetic operation program comprising:

an acquiring step performed by the acquiring means, for acquiring affine coordinates of at least one point on the elliptic curve E and operation information indicating one of the addition and the doubling, from an external source;

a transforming step performed by the transforming means, for performing a 11 coordinate transformation on the acquired affine coordinates to generate Jacobian coordinates, 12 the coordinate transformation being transforming affine coordinates $(\phi (\alpha), \beta x \phi(\alpha))$ of a given 13 point on the elliptic curve E using polynomials 14

15
$$X(\alpha) = f(\alpha)x\phi(\alpha)$$

16
$$Y(\alpha) = f(\alpha) \{ 2x\varphi (\alpha) \}$$

$$17 Z(\alpha) = I$$

into Jacobian coordinates $(X(\alpha):Y(\alpha):\beta xZ(\alpha)), \phi(\alpha)$ and $\phi(\alpha)$ being polynomials; 18

19 and

20

21

22

3

an operating step performed by the operating means, for performing one of the addition and the doubling indicated by the acquired operation information, on the generated Jacobian coordinates to obtain Jacobian coordinates of a point on the elliptic curve E.

- (Original) The storage medium of Claim 25, wherein the acquiring step 1 26.
- in a first case acquires affine coordinates of two different points on the 2 (a) elliptic curve E and operation information indicating the addition, and
- in a second case acquires affine coordinates of a single point on the elliptic 4 (b) 5 curve E and operation information indicating the doubling,
- 6 wherein the transforming step
- in the first case performs the coordinate transformation on the acquired 7 (a) affine coordinates of the two different points to generate Jacobian coordinates of the two 8 9 different points, and
- in the second case performs the coordinate transformation on the acquired 10 (b) affine coordinates of the single point to generate Jacobian coordinates of the single point, and 11

12	wherein the operating step
13	(a) in the first case performs the addition indicated by the acquired operation
14	information on the generated Jacobian coordinates of the two different points to obtain the
15	Jacobian coordinates of the point on the elliptic curve E , and
16	(b) in the second case performs the doubling indicated by the acquired
17	operation information on the generated Jacobian coordinates of the single point to obtain the
18	Jacobian coordinates of the point on the elliptic curve E .
1	27. (Currently Amended) The storage medium of Claim 26, wherein in the first case
2	the acquiring step acquires affine coordinates
3	$\frac{(XI(\alpha), \ \beta xYI(\alpha))}{(\phi_l(\alpha), \ \beta x \varphi_l(\alpha))}$
4	$\frac{(X_2(\alpha), \beta x Y_2(\alpha))}{(\phi_2(\alpha), \beta x \varphi_2(\alpha))}$
5	of the two different points on the elliptic curve E and the operation information
6	indicating the addition,
7	the transforming step performs the coordinate transformation on the acquired
8	affine coordinates of the two different points to generate Jacobian coordinates
9	$(XI(\alpha):YI(\alpha):\beta xZI(\alpha))$
10	$(X2(\alpha):Y2(\alpha):\beta xZ2(\alpha))$
11	of the two different points, and
12	the operating step computes
13	$U1(\alpha) = X1(\alpha)xZ2(\alpha) \{ 2 \}$
14	$U2(\alpha) = X2(\alpha)xZI(\alpha) \{ 2$
15	$SI(\alpha) = YI(\alpha)xZ2(\alpha)$ { 3
16	$S2(\alpha) = Y2(\alpha)xZI(\alpha) \{ 3 \}$

17
$$H(\alpha) = U2(\alpha) - U1(\alpha)$$
18 $r(\alpha) = S2(\alpha) - S1(\alpha)$
19 and computes
20 $X3(\alpha) = -H(\alpha) \{ 3-2xU1(\alpha)xH(\alpha) \{ 2+r(\alpha) \} \}$
21 $Y3(\alpha) = -S1(\alpha)xH(\alpha) \{ 3+r(\alpha)x(U1(\alpha)xH(\alpha) \} \}$
22 $Z3(\alpha) = Z1(\alpha)xZ2(\alpha)xH(\alpha)$
23 to obtain Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the elliptic
24 curve E.

1 28. (Currently Amended) The storage medium of Claim 26,
2 wherein in the second case the acquiring step acquires affine coordinates
3 $(X1(\alpha) - \beta xY1(\alpha)) \cdot (\phi_1 \cdot (\alpha) - \beta x\phi_1(\alpha))$
4 of the single point on the elliptic curve E and the operation information indicating
5 the doubling,
6 the transforming step performs the coordinate transformation on the acquired
7 affine coordinates of the single point to generate Jacobian coordinates
8 $(X1(\alpha) : Y1(\alpha) : \beta xZ1(\alpha))$
9 of the single point, and
10 the operating step computes
11 $S(\alpha) = 4xX1(\alpha)xY1(\alpha) \{ 2 \}$
12 $M(\alpha) = 3xX1(\alpha) \{ 2+axZ1(\alpha) \} \{ 4xf(\alpha) \} \{ 2 \}$
13 $T(\alpha) = -2xS(\alpha) + M(\alpha) \} \{ 2 \}$

and computes 14 $X3(\alpha) = T(\alpha)$ 15 $Y3(\alpha) = -8xYI(\alpha) \left\{ 4 + M(\alpha)x(S(\alpha) - T(\alpha)) \right\}$ 16 $Z3(\alpha) = 2xYI(\alpha)xZI(\alpha)$ 17 to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta xZ3(\alpha))$ of the point on the elliptic 18 19 curve E. (Currently Amended) The storage medium of Claim 26, 29. 1 wherein the acquiring step 2 in the first case acquires affine coordinates 3 (a) $(XI(\alpha), \beta xYI(\alpha))$ $(\phi_I(\alpha), \beta x \phi_I(\alpha))$ 4 $(X2(\alpha), \beta x Y 2(\alpha))$ $(\phi_2(\alpha), \beta x \phi_2(\alpha))$ 5 of the two different points on the elliptic curve E and the operation information 6 indicating the addition, and 7 in the second case acquires affine coordinates 8 (b) $(XI(\alpha), \beta xYI(\alpha))$ $(\phi_1(\alpha), \beta x \phi_1(\alpha))$ 9 of the single point on the elliptic curve E and the operation information indicating 10 11 the doubling, 12 wherein the transforming step in the first case performs the coordinate transformation on the acquired (a) 13 14 affine coordinates of the two different points to generate Jacobian coordinates $(X1(\alpha):Y1(\alpha):\beta xZ1(\alpha))$ 15 $(X2(\alpha):Y2(\alpha):\beta xZ2(\alpha))$ 16 of the two different points, and 17

in the second case performs the coordinate transformation on the acquired 18 (b) 19 affine coordinates of the single point to generate Jacobian coordinates 20 $(XI(\alpha):YI(\alpha):\beta xZI(\alpha))$ of the single point, and 21 22 wherein the operating step (a) in the first case computes 23 $UI(\alpha) = XI(\alpha)xZ2(\alpha)$ { 2 24 $U2(\alpha) = X2(\alpha)xZ1(\alpha)$ { 2 25 $SI(\alpha) = YI(\alpha)xZ2(\alpha)$ { 3 26 27 $S2(\alpha) = Y2(\alpha)xZ1(\alpha)$ { 3 28 $H(\alpha) = U2(\alpha) - U1(\alpha)$ $r(\alpha) = S2(\alpha) - S1(\alpha)$ 29 30 and computes $X3(\alpha) = -H(\alpha) \left\{ 3 - 2xUI(\alpha)xH(\alpha) \right\} \left\{ 2 + r(\alpha) \right\} \left\{ 2 + r(\alpha) \right\}$ 31 $Y3(\alpha) = -S1(\alpha)xH(\alpha) \{ 3+r(\alpha)x(U1(\alpha)xH(\alpha) \} \{ 2-X3(\alpha) \}$ 32 $Z3(\alpha) = Z1(\alpha)xZ2(\alpha)xH(\alpha)$ 33 to obtain Jacobian coordinates $(X3(\alpha):Y3(\alpha):\beta xZ3(\alpha))$ of the point on the elliptic 34 35 curve E, and 36 (b) in the second case computes $S(\alpha) = 4xXI(\alpha)xYI(\alpha)$ { 2 37 38 $M(\alpha) = 3xXI(\alpha) \{ 2 + axZI(\alpha) \} \{ 4xf(\alpha) \}$ $T(\alpha) = -2xS(\alpha) + M(\alpha) \{ 2 \}$ 39

and computes $X3(\alpha) = T(\alpha)$ $Y3(\alpha) = -8xYI(\alpha) \left\{ 4 + M(\alpha) x(S(\alpha) - T(\alpha)) \right\}$ $Z3(\alpha) = 2xYI(\alpha)xZI(\alpha)$ 44 to obtain the Jacobian coordinates $(X3(\alpha) : Y3(\alpha) : \beta xZ3(\alpha))$ of the point on the
45 elliptic curve E.

1 30-33. (Cancelled)